WHAT IS CLAIMED IS:

1. In an Internet, a network-based mobile workgroup system providing limited access for a selected set of initiating parties to an equally limited set of target parties, available in one or more mobile virtual private networks (M-VPNs) with possibly overlapping address realms.

2. The network-based mobile workgroups of claim 1, wherein the access restrictions are performed by a realm-indexed workgroup filter in the ingress security gateway of the mobile virtual private network containing the target party for a unidirectional stream of datagrams.

3. The realm-indexed workgroup filtering technique of claim 2, wherein a security gateway of a mobile virtual private network has at least one public IP address that is unique within the Internet.

4. The realm-indexed workgroup filtering technique of claim 3, wherein the security gateway of the initiating party is establishing an IP-IP tunnel to the security gateway of the target party using public IP addresses.

5. The realm-indexed workgroup filtering technique of claim 4, wherein the initiating party retrieves the user fully qualified domain name and private IP address of the target party as well as the public IP address of the target party's security gateway when signing on to an extranet workgroup or when the membership list at the mobile service manager portal is updated.

6. The realm-indexed workgroup filtering technique of claim 5, wherein the target party security gateway applies the source IP address of the IP-IP tunnel as an index for the initiating party's private IP address in the workgroup filter table.

7. The realm-indexed workgroup filtering technique of claim 6, wherein a unidirectional IPSec tunnel is established for sending datagrams from the initiating party to the target party's security gateway.

8. The unidirectional IPSec tunnel of claim 7, wherein the security association between the initiating party and the target party's security gateway is established using the Internet Key Exchange protocol.

9. The Internet Key Exchange protocol of claim 8, wherein the initiating party and the target party's security gateway exchange X.509 certificates as part of the Internet Key Exchange procedure.

10. The X.509 certificates of claim 9, wherein the initiating party's certificate includes its security gateway public IP address as part of the Subject Alternative Name field.

11. The X.509 certificate extension of claim 10, wherein the target party's security gateway matches the Subject Alternative Name field with the source IP address of the IP-IP tunnel in order to uniquely select the security association for incoming IPsec datagrams with source IP address equal to the initiating party's private IP address.

12. The realm-indexed workgroup filtering technique of claim 2, wherein the same technique is applied between the target party and the initiating party's security gateway for datagrams sent in the direction from target to initiating party.

13. The reverse path procedure of claim 12, wherein the target party retrieves the user fully qualified domain name and private IP address of the initiating party as well as the public IP address of the initiating party's security gateway when signing into an extranet workgroup or updating the member list at the mobile service manager portal.

14. The network-based mobile workgroups of claim 1, wherein inter-domain mobility between mobile virtual private networks is performed using mobile IP and intra-domain mobility within each mobile virtual private network is performed using mobility routing.

15. The inter-domain mobility solution of claim 14, wherein the security gateway of each mobile virtual private network also act as home agent for its local mobile nodes.

16. The inter-domain mobility solution of claim 15, wherein security gateways for several mobile virtual private networks are implemented as virtual home agents in the same operator-based physical home agent.

17. The operator-based home agent of claim 16, wherein an integrated dispatcher is distributing datagrams to the virtual home agents based on IP tunnel destination IP address.

18. The operator-based home agent of claim 16, wherein a foreign agent on a public access network may be shared by multiple virtual home agents with overlapping home network IP address realms.

19. The operator-based home agent of claim 18, wherein the virtual home agents share a common backbone virtual router for sending traffic towards the Internet.

20. The operator-based home agent of claim 19, wherein the common backbone virtual router hosts a mobile service manager with a public IP address.

21. The operator-based home agent of claim 20, wherein the mobile service manager hosts a domain name server for the mobile workgroup system.

22. The operator-based home agent of claim 21, wherein the common backbone virtual router contains a network address port translator for accepting portal request/replies from a mobile node in a particular mobile virtual private network to the mobile service manager.

23. The inter-domain mobility solution of claim 15, wherein the mobile node is applying the mobile IP co-located care-of address scenario in case no foreign agent is available on the visited subnetwork.

24 The co-located care of address scenario of claim 23, wherein the mobile node establishes an extra IPSec tunnel to its home agent inside the mobile IP tunnel and outside the realm-indexed workgroup IPSec tunnel.

25. The intra-domain mobility solution of claim 14, wherein the mobility routing protocol is the Ad-hoc On-demand Distance Vector (AODV) protocol.

26. The intra-domain mobility solution of claim 25, wherein AODV is extended with a proactive routing update for active peers at handover of mobile node between old and new sinks (ingress mobility routers).

27. The handover mechanism of claim 26, wherein the mobile node sends a hello message to its newly discovered sink with a destination sequence number set equal to the destination sequence number of the last registration reply that was distributed via the old sink.

28. The handover mechanism of claim 27, wherein the new sink takes this first hello message as an indication that it now is asked to take the role of new sink in the core mobility router network for the mobile node.

29. The handover mechanism of claim 28, wherein the new sink directly sends an unsolicited route reply in the direction towards the old sink, if it has an existing route towards the mobile node in its routing table and the destination sequence number is the same for this route as the one received from the mobile node in the hello message.

30. The handover mechanism of claim 29, wherein the new sink sends a route request with the destination sequence number set to the same value as received from the mobile node in the hello message.

31. The handover mechanism of claim 30, wherein the old sink, or any mobility router along the path to the old sink, will respond with a route reply message.

32. The handover mechanism of claim 31, wherein the new sink sends an unsolicited route reply message for the mobile node destination with the route request source IP address set to the old sink and the destination sequence number incremented by one.

33. The handover mechanism of claim 32, wherein the old sink and all mobility routers along the path between the old and the new sink are updated with the new route having a better destination sequence number.

34. The handover mechanism of claim 33, wherein the old sink will forward all packets destined to the mobile node along the route via the new sink.

35. The handover mechanism of claim 34, wherein a route reply is sent from the old sink via the new sink to the mobile node to indicate that the handover procedure has been successful, alternatively that the new sink sends a route error to the mobile node if it cannot reach the old sink.

36. The handover mechanism of claim 35, wherein the mobile node now can migrate datagram forwarding from the link of the old sink to the link of the new sink.

37. The handover mechanism of claim 36, wherein at successful handover procedure the mobile node may at its leisure decide to optimize the path towards active peers, by initiating route requests towards those destinations; while route requests are sent immediately towards active peers in case of a unsuccessful handover procedure.

38. The route optimization mechanism of claim 37, wherein the source sequence number in the route request to an active peer is set equal to the new destination sequence number of the mobile node.

39. The route optimization mechanism of claim 38, wherein the route replies of the route request establishes a bi-directional, optimal path between the mobile node and his peer.

40. The intra-domain mobility solution of claim 14, wherein the mobile node sends an authentication extension to the new sink in its hello message.

41. The security solution of claim 40, wherein the new sink sends a DIAMETER query, based on the incoming AODV routing protocol authentication extension, to the home network mobile service manager in order to perform central authentication and receive static routes and workgroup filters to be applied to traffic from/to the mobile node.

42. The security solution of claim 41, wherein the subnetwork may span multiple sites interconnected via IPSec gateways.

43. The security solution of claim 42, wherein one static route received is the default route of the subnetwork and another static route is the home network IP address range having a lower cost than the default route.

44. The security solution of claim 43, wherein the sink advertises the default route and the home network IP address range to the mobile node if the authentication is successful, i.e. the mobile node belongs to the home network and is registered in the local mobile service manager.

45. The security solution of claim 44, wherein a mobile node belonging to the local mobile virtual private network is using the default route as an address to the security gateway towards the Internet/other mobile virtual private networks and applies it only for addresses that are outside the address range allocated to the home network.

46. The security solution of claim 45, wherein a visiting mobile node, not belonging to the local mobile virtual private network and therefore not successfully authenticated by the local mobile service manager, is only sent the default route with a gateway address equal to the foreign agent IP address.

47. The security solution of claim 46, wherein the visiting mobile node after unsuccessful authentication establishes an IP-IP or IPSec tunnel to the foreign agent that is given by the default route.

48. The IP-IP tunnel of claim 47, wherein the source address of the inner IP header is the private IP address of the visiting mobile node as given by the home mobile virtual private network and the source address of the outer IP header is the private or public IP address of the visiting mobile node as allocated by the visited mobile virtual private network.

49. The security solution of claim 48, wherein the sink of the visiting mobile node only allows traffic tunneled from/to the foreign agent to pass the local workgroup filter.

50. The security solution of claim 40, wherein a public key infrastructure is used for mobile node authentication.

51. The security solution of claim 50, wherein the mobile node piggybacks its X.509 certificate in the initial hello message (exemplified by an AODV route reply) to the mobile service router acting as sink.

52. The security solution of claim 51, wherein the sink verifies that the certificate is signed by the mobile service manager and uses the public key of the received certificate to authenticate the mobile node.

53. The security solution of claim 52, wherein the sink sends its certificate to the mobile node.

54. The security solution of claim 53, wherein the mobile node verifies that the certificate is signed by the mobile service manager and uses the public key of the received certificate to authenticate the mobile service router acting as new sink.

55. The security solution of claim 54, wherein the own and mobile service manager certificate is retrieved by the mobile nodes and the mobile services routers from the mobile service manager as part of management configuration.

55. The security solution of claim 50, wherein the mobile node certificate is retrieved by the mobile services router from the mobile service manager as a domain name system query triggered by the initial hello message.

56. The security solution of claim 50, wherein the mobile node certificate is retrieved by the mobile services router from the mobile service manager as a DIAMETER query triggered by the initial hello message.

57. The intra-domain mobility solution of claim 25, wherein the mobile service router sink for a mobile node also acts as a proxy for all mobility routing protocol exchanges for the mobile node towards the network.

58. The mobility routing proxy solution of claim 57, wherein the mobile node uses a Dynamic Host Configuration Protocol (DHCP) request as its hello message to a new sink.

59. The mobility routing proxy solution of claim 58, wherein the mobile node includes its IP address and authenticator as part of the DHCP request.

60. The mobility routing proxy of claim 59, wherein the mobile service router sink, maps the DHCP request to a DIAMETER request sent to the mobile service manager for authentication.

61. The mobility routing proxy of claim 60, wherein the mobile service router sink initiates a route request on behalf of the mobile node when receiving a datagram from the mobile node.

62. The mobility routing proxy of claim 61, wherein the mobile service router sink buffers the received datagrams until a path is established to the destination.

63. The intra-domain mobility solution of claim 25, wherein weights are assigned to neighbor hops in order to limit broadcast route requests using when applying expanding ring search in AODV.

64. The weight-controlled expanding ring search of claim 63, wherein the weight for a hop can be administratively configured on the mobile service router.

65. The weight-controlled expanding ring search of claim 64, wherein the sum of weights from the source IP address of the request to the mobile service router handling the request is used to select path.

66. The weight-controlled expanding ring search of claim 65, wherein the mobile service routers to send an expanding ring search route request to is limited to the ones with the lowest sum of weights from the source IP address of the request to the candidate neighbor mobile service router.

67. The intra-domain mobility solution of claim 25, wherein the source of a route reply may proactively initiate a gratuitous route reply towards a source of a route request in order to provide continuous streaming of datagrams for active sessions.

68. The gratuitous route reply of claim 67, wherein the source of a route reply sends the gratuitous route reply if the life time of the route is running out within a configured number of seconds and datagrams are received along the path.

69. The gratuitous route reply of claim 68, wherein the configured number of seconds left on the route lifetime triggering gratuitous route reply from the route reply source is larger than the configured number of seconds left on the route lifetime triggering a new route request from the route request source.

70. The gratuitous route reply of claim 68, wherein the gratuitous route reply is being unicast along the spanning tree already created for the active sessions towards the destination.